

Manual da ***Due Diligence***

Manual de apoio para preenchimento de avaliações de continuidade de negócios, privacidade e segurança da informação.

ICATU

CONTEÚDO

- [1. Este manual](#)
- [2. Diretrizes de preenchimento](#)
- [3. Recebendo o formulário](#)
- [4. Acessando a plataforma](#)
- [5. Conhecendo as seções](#)
- [6. Navegando pelos blocos](#)
- [7. Respondendo às avaliações](#)
 - [7.1. Continuidade de Negócios](#)
 - [7.1.1. Perguntas objetivas](#)
 - [7.1.2. Anexando evidências](#)
 - [7.2. Privacidade](#)
 - [7.2.1. Perguntas objetivas](#)
 - [7.2.2. Perguntas discursivas](#)
 - [7.3. Segurança da Informação](#)
 - [7.3.1. Diligência simplificada](#)
 - [7.3.2. Diligência completa](#)
- [8. Finalizando a diligência](#)
- [9. Diligência devolvida](#)
- [10. Solicitação de informações](#)
- [11. Reenviando o formulário](#)
- [12. Perguntas frequentes](#)



Este manual

Este manual foi elaborado para ajudar empresas prestadoras de serviços ou fornecedores de produtos para o **Grupo Icatu** a concluir a etapa de *due diligence* da contratação.

O que é uma *due diligence*? É uma avaliação que o **Grupo Icatu** realiza para apurar se uma empresa segue o disposto na lei, em regulamentos específicos e/ou se possui processos, medidas e controles relacionados aos temas que são importantes para o **Grupo Icatu**. A *due diligence* se apresenta no formato de questionário, que é respondido na plataforma *online* [OneTrust](#).

A quem se destina? A todas as pessoas físicas ou jurídicas, fornecedores de produtos ou prestadores de serviços (**Sua Empresa**) que tiverem interesse em ser contratados pelo **Grupo Icatu**.

Por que ela é importante? Porque permite que o **Grupo Icatu** conheça a **Empresa**, entendendo como ela contribui para a continuidade dos nossos negócios, como se posiciona em matéria de proteção de dados pessoais e como seu polo de tecnologia se desenvolve, a partir de regramentos técnicos para a garantia da segurança das informações.





Diretrizes de preenchimento

Conforme o quadro abaixo, é possível receber mais de um questionário.

	Avaliaremos	Com o objetivo de	Importante observar
Continuidade de Negócios	Como Sua Empresa e seus produtos contribuem para a continuidade dos negócios do Grupo Icatu	Conhecer a maturidade de Sua Empresa no que tange à gestão de continuidade de negócios, ao cumprimento da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018) e à verificação de requisitos mínimos e ações recomendadas para defesa cibernética	As diligências focarão em Sua Empresa como um todo não apenas o serviço para o qual Você a está cadastrando, nem o papel de Sua Empresa enquanto agente de tratamento de dados.
Privacidade	O Programa de Privacidade de Sua Empresa		
Segurança da Informação	Os requisitos mínimos para garantir a Segurança da Informação se o produto ou serviço envolvem interação tecnológica, manipulação de informação ou desenvolvimento de solução tecnológica .		



Sempre forneça respostas **completas** e apresente **evidências** de suas afirmações, a fim de evitar [Solicitações de Informações](#) adicionais por parte do **Grupo Icatu**.



Clique nos links para ir direto à seção das avaliações

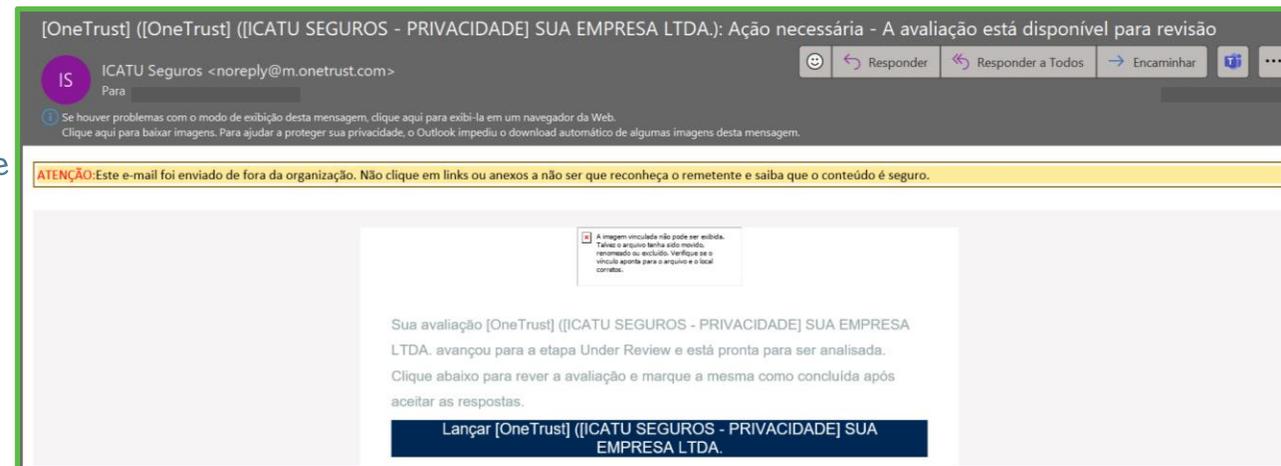
Recebendo o formulário



Caso **Você** tenha sido apontado/a como respondente da diligência, enviaremos o questionário ao seu endereço de email. **Você** receberá uma mensagem:

- **Do Remetente:** ICATU Seguros noreply@m.onetrust.com
- **Com o assunto no formato:** [OneTrust] ([ICATU SEGUROS – NOME DA AVALIAÇÃO] – NOME DA SUA EMPRESA): Ação necessária - A avaliação está disponível para revisão

Neste exemplo, a avaliação enviada é a de Privacidade

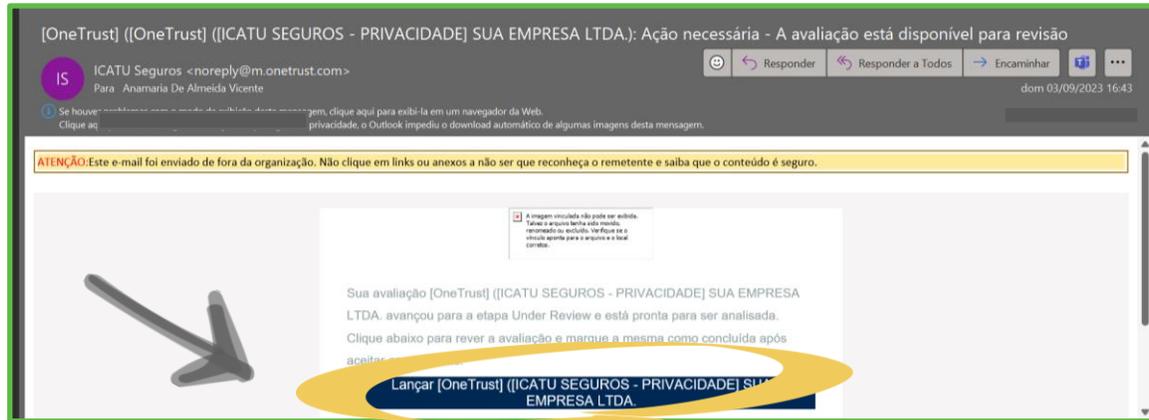


Caso não tenha recebido o e-mail na sua caixa de entrada, favor verificar sua lixeira ou caixa de spam.

Acessando a plataforma



Clicando no *link* azul da mensagem, **Você** será direcionado para o ambiente OneTrust.



Se **Você** foi indicado como respondente, será redirecionado para cá. A ferramenta não exige senha de usuários cadastrados. Confira seu email e clique em “**Seguinte**”.



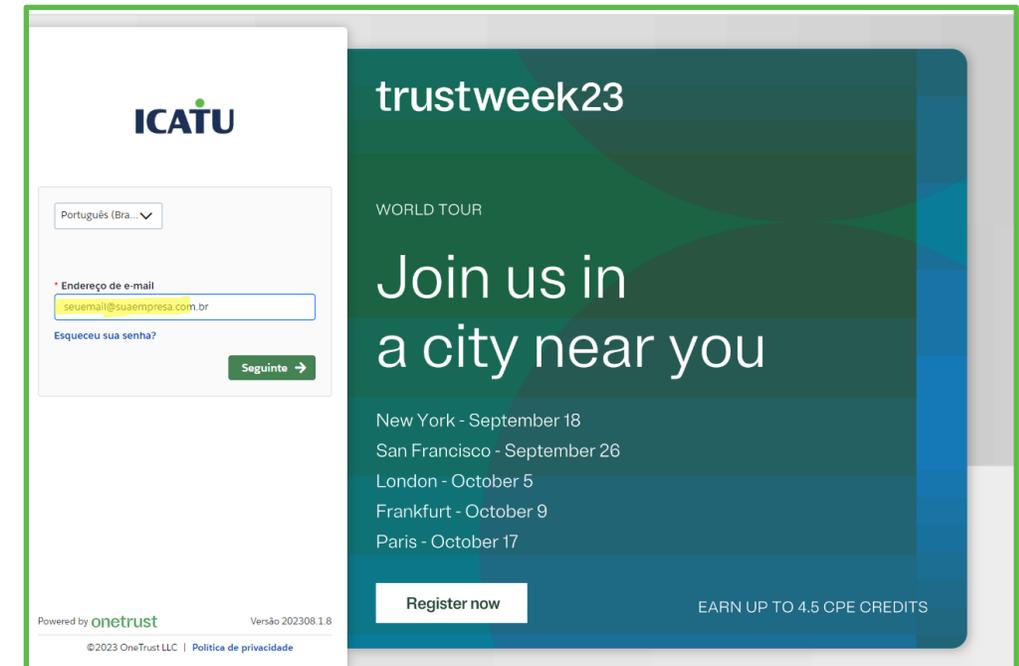
Evite encaminhar o email a outras pessoas. Só pessoas cadastradas como respondente consegue acessar o formulário. Se necessário incluir outros respondentes, acione seu contato no **Grupo Icatu** e faça este pedido.



Os respondentes devem conhecer o assunto dentro de **Sua Empresa** para que a aprovação aconteça de modo ágil e produtivo. Indique como respondentes pessoas que conheçam dos temas continuidade de negócios, segurança da informação e privacidade.



A partir da data de envio, **Sua Empresa** terá até 7 (sete) dias úteis para enviar o formulário.



Conhecendo as seções



Aqui **Você** vê os anexos que incluiu

Aqui estão todas as Solicitações de Informações, onde **Você** pode ver os novos esclarecimentos que pedimos

[OneTrust] [ICATU SEGUROS - ...] Não iniciada 1/6 17%

NÃO INICIADA EM ANDAMENTO SOB REVISÃO CONCLUÍDO

Privacidade - Avaliação de Fornecedores

Selecionar um idioma

Mostrar: Todas as perguntas

Boas-vindas

Bloco 1 - Perguntas gerais sobre o fornecedor

Bloco 2 - Perguntas sobre o Programa de Privacidade do Fornecedor

Bloco 3 - Perguntas sobre o atendimento ao titular de dados

Bloco 4 - Perguntas

Bem-vindo(a) ao nosso Portal de Gestão de Risco de Fornecedores!

Esta avaliação tem por objetivo identificar o grau de maturidade das empresas que prestam ou pretendem prestar serviços ao Grupo Icatu Seguros, Icatu Vanguarda e Icatu Fundo Multipatrocinado - Icatu FMP ("Icatu") sob a ótica de proteção de dados pessoais, com base na Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018) e em boas práticas de mercado sobre o tema.

Você foi indicado(a) como ponto focal para responder as questões de privacidade e proteção de dados em nome da sua empresa. Para melhor entendimento, seguem abaixo alguns conceitos importantes previstos na LGPD:

- a) **Dado Pessoal** = toda informação relacionada a pessoa natural (pessoa física) identificada ou identificável, ou seja, que permita a sua identificação (exemplo: nome, CPF, matrícula, documentos de identidade, endereço, informações financeiras etc.);
- b) **Dado Pessoal Sensível** = todo dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; e
- c) **Tratamento de Dados Pessoais** = é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Lembre-se: Todas e quaisquer perguntas neste formulário são imprescindíveis para a avaliação da Icatu e precisam, portanto, ser respondidas exaustivamente.

Recursos de comentários são integrados a este portal. Você pode sinalizar suas dúvidas clicando no ícone de 'chat' que fica abaixo de cada questão. Adicionalmente, comentários orientam nossa equipe, que fornecerá ajuda diretamente nesta ferramenta. Você também pode anexar documentos e/ou evidências, caso necessário, clicando no botão de 'anexo' localizado abaixo das questões.

Aqui estão todos os comentários eventualmente inseridos por **Você** ou pelo **Grupo Icatu**.

Nesta coluna à esquerda estão todos os **blocos** em que o questionário se divide.

Boas-Vindas: aqui inserimos conceitos-chave e orientações sobre como preencher o formulário



Navegando pelos blocos

Privacidade - Avaliação de Fornecedores

Selecione um idioma. ▾

Mostrar: Todas as perguntas ▾

Boas-vindas

Bloco 1 - Perguntas gerais sobre o fornecedor >

Bloco 2 - Perguntas sobre o Programa de Privacidade do Fornecedor >

Bloco 3 - Perguntas sobre o atendimento ao titular de dados >

[ICATU] - Controles - Avaliação de Segurança para Fornecedores e Parceiros

Selecione um idioma. ▾

Mostrar: Todas as perguntas ▾

Boas-vindas

Básico ▾

1.1 CIS 20 - Cyber Security Framework

* 1.2 Existe um indivíduo / grupo designado para supervisionar o programa de segurança de informações /

Continuidade do Negócio - Avaliação de Fornecedores

Selecione um idioma. ▾

Mostrar: Todas as perguntas ▾

Boas-vindas

1. Infraestrutura >

2. Processo GCN >

Cada diligência possui um conjunto de blocos.

Se houver uma sinalização em vermelho, como no exemplo ao lado, significa que há perguntas sem respostas. Todas as perguntas devem ser respondidas, do contrário não será possível finalizar o questionário e enviá-lo de volta ao **Grupo Icatu**.



Mostrar: Todas as perguntas ▾

Boas-vindas

Avaliação de Certificado de Segurança * >

CIS 18: Testes de Invasão * >



O salvamento de cada questionário é automático, mas se preferir, **Você** pode clicar em “Salvar e Sair”, retornando ao questionário posteriormente.

▶ Ao final de cada bloco, no rodapé de cada página, basta clicar no ícone “>” para avançar para o bloco seguinte.

Próxima seção

< >

Salvar e sair Enviar

Respondendo a diligência de

Continuidade de Negócios



Perguntas objetivas

Nas avaliações de Continuidade de Negócios, há dois blocos de perguntas: “Infraestrutura” e “Processo GCN”.

Todas as perguntas da avaliação de continuidade de negócios são objetivas. Abaixo de cada pergunta, há sempre uma explicação. Leia a explicação, juntamente com a pergunta. Caso seja necessário, **Você** poderá inserir um comentário a respeito de sua resposta.

Exemplo de pergunta do bloco “Infraestrutura”

1.2 *O fornecedor possui uma estrutura e/ou recursos alocados para as atividades de contingência e/ou continuidade dos serviços contratados ou a serem contratados?

O fornecedor deve ter uma estrutura mínima de continuidade e/ou contingência nas atividades de GCN, inclusive traduzida na estrutura corporativa.

0 0



Utilize o balão de comentários a seu favor, sempre que precisar fornecer justificativas sobre a maturidade e os controles de **Sua Empresa**.

Exemplo de pergunta do bloco “Processos GCN”

2.2 *O fornecedor possui um plano de contingência/recuperação de crises, formalizado, que mitigue os possíveis Impactos no caso de interrupção dos serviços contratados ou a serem contratados?

O fornecedor deve possuir planos de contingência/recuperação de crises formalizados.

0 0

Anexando evidências



Há, no bloco “Processos GCN”, uma pergunta em que o **Grupo Icatu** solicita evidência de que **Sua Empresa** realiza Testes de Simulação. Se sua resposta for positiva, na pergunta seguinte, é solicitada uma evidência de sua realização. O **Grupo Icatu** solicita esta evidência a fim de garantir a eficiência do ambiente de controle de GCN.

Esta providência é essencial para que o **Grupo Icatu** avalie se **Sua Empresa** realiza exercícios periódicos que simulem a interrupção e recuperação dos processos que suportam os serviços contratados ou a serem contratados.

Pergunta sobre Teste de Simulação

2.3 *O fornecedor realiza exercícios/testes periódicos que simulem a interrupção e recuperação dos processos que suportem os serviços contratados ou a serem contratados?

O fornecedor deve possuir uma rotina de testes periódica (no mínimo anual) para garantir a eficiência do ambiente de controle de GCN.

Favor, evidenciar a realização de Testes de Simulação através de relatório com o resultado dos exercícios/testes, podendo ser uma cópia do índice e/ou sumário do relatório, com o campo de assinaturas devidamente assinados

1 2

2.4 *Anexo

1

Se a resposta foi “Sim” mas nenhuma evidência foi anexada, o questionário poderá ser devolvido, gerando novos questionamentos do **Grupo Icatu**.

Portanto, se **Sua Empresa** realizar testes de simulação, eles deverão ser documentados.

Caso contrário, solicitamos alterar a resposta para “Não”, a fim de evitar atrasos desnecessários na avaliação.

Respondendo a diligência de
Privacidade

Perguntas objetivas



A diligência de Privacidade contém cinco blocos de perguntas relacionadas ao Programa de Privacidade de **Sua Empresa**. Há perguntas que podem ser respondidas com “Sim” ou “Não” e outras que demandam respostas discursivas.

Quando a pergunta for respondida com “Sim”, normalmente, na pergunta seguinte, solicitamos justificar a resposta ou anexar evidências, que podem ser apresentadas nos formatos PDF, JPG, XLS, DOC, dentre outros.

2.1 *O fornecedor já designou um Encarregado pelo Tratamento de Dados (DPO)?



2.2 Pedimos fornecer o nome e o e-mail de contato do Encarregado pelo Tratamento de Dados (DPO).

2.7 *O fornecedor possui políticas publicadas e procedimentos vigentes para garantir o cumprimento de seu programa de privacidade?



2.8 Favor fornecer uma cópia de seu Aviso/Política de Privacidade, documento através da qual é cumprida a obrigação prevista no art. 9º da LGPD.

2.18 *O fornecedor possui registro das operações de tratamento de dados pessoais (RoPA), conforme exigido pelo art. 37 da LGPD?



2.19 Favor fornecer uma cópia do modelo do registro das operações de tratamento de dados pessoais (RoPA).

Caso o fornecedor tenha implantado seu registro de operações de tratamento por meio de documentos (relatórios, formulários), pedimos uma cópia deste documento, com um processo de negócio preenchido.



Perguntas discursivas

Quando a pergunta for discursiva, cabe a **Você** fornecer respostas completas e detalhadas.

Abaixo de cada pergunta, há sempre uma explicação. Leia-a juntamente com a pergunta e busque fornecer respostas completas e relacionadas ao que foi questionado. Isso ajudará o **Grupo Icatu** a avaliar **Sua Empresa** da maneira mais diligente e justa, deixando de atribuir riscos desnecessários. Veja os exemplos abaixo:

1.2 *Quais são os produtos/serviços que o fornecedor oferece?

Precisamos saber quais serviços e/ou produtos sua empresa possui capacidade técnica e/ou autorização legal para ofertar.

Serviços de marketing



1.2 *Quais são os produtos/serviços que o fornecedor oferece?

Precisamos saber quais serviços e/ou produtos sua empresa possui capacidade técnica e/ou autorização legal para ofertar.

MINHA EMPRESA presta serviços de soluções de marketing, tais como peças publicitárias, marketing de conteúdo, elaboração de apresentações, desenho de produto, desenho de campanhas, análise de dados, CRM analítico, dentre outras atividades de inteligência de mercado.



Dê respostas assertivas, que permitam ao **Grupo Icatu** entender o grau de maturidade e **Sua Empresa** e quais controles ela adota para atender a legislação. Respostas vagas e curtas farão com que o **Grupo Icatu** solicite [informações adicionais](#), o que pode gerar atrasos na conclusão desta etapa.

Respondendo a diligência de

Segurança da Informação

Diligência simplificada



Há dois tipos de diligência de Segurança da Informação.

O primeiro é composto pela verificação de certificados de segurança, sendo eles **SOC2**, **ISO27001** ou **PCI**, que sejam válidos para o escopo do contrato. Caso **Sua Empresa** possua um certificado, basta responder positivamente à pergunta 1.2, indexar a evidência na pergunta 1.3 e retornar a avaliação, conforme indicado na seção [Finalizando a diligência](#).

1.2 * Possui certificação SOC2, ISO27001 ou PCI e o serviço a ser prestado está incluído no escopo dessa certificação?

Sim Não

0 0



1.3 * Anexe o certificado SOC2, ISO27001 ou PCI correspondente:

OBS: Não aceitaremos certificado fora do prazo de vigência.

Essa pergunta requer um anexo

* 0



Recomendamos a leitura do tópico [Boas-Vindas](#) no questionário enviado via Onetrust para esclarecer eventuais dúvidas de preenchimento.

Diligência completa



Se **Sua Empresa** não possui certificado ou se o **Grupo Icatu** identificar que o documento não é válido para o escopo, as perguntas que estavam ocultas serão ativadas, e seu preenchimento será obrigatório. Para cada pergunta, conforme apontado abaixo:

Implementado: ao selecionar esta opção, uma nova questão será aberta para anexar a evidência da implementação do controle

3.1 *Possui inventário detalhado de ativos de hardware?
Apresentar Inventário detalhado de todos os ativos de hardware corporativos que armazenam ou processam dados.

Implementado Não Implementado
Em planejamento



3.2 *Anexe a evidência que comprove a implementação do controle:
Favor anexar a evidência.

* 1 É obrigatório anexar a evidência.

Em planejamento: selecionando-a, abre-se uma nova questão para informar qual a data de previsão de implementação do controle

Implementado Não implementado
Em planejamento



3.3 *Informe qual a data de previsão de implementação do controle:

Escolha uma data

0 0

É obrigatório informar a data prevista para implementação

Não Implementado: ao selecionar esta opção, não é necessário anexar nenhuma evidência

Implementado **Não implementado**
Em planejamento

Etapas
Finais

Finalizando a diligência



Antes de finalizar, confirme se todas as perguntas possuem resposta. A sinalização “*00” [conforme figura ao lado de cada bloco] indica que ainda há perguntas sem respostas. Se esta sinalização estiver marcada, **Você** não conseguirá enviar o questionário ao **Grupo Icatu**.



Não havendo nenhuma pergunta em aberto, será habilitado o botão verde “**Enviar**”.



Importante: não basta responder a todas as perguntas, é preciso clicar em “**Enviar**”. Do contrário, o **Grupo Icatu** não receberá as respostas e não poderá dar andamento à avaliação.

Diligência devolvida



Se, depois de responder a diligência, **Você** receber outro email da OneTrust, será porque, ao avaliar as respostas, o **Grupo Icatu** pediu informações complementares ou evidências que não foram atendidas [ou foram atendidas de modo incompleto].

Será necessário repetir o procedimento das primeiras etapas: clicar no *link* do *email*, abrir o formulário, avaliar as “[Solicitação de Informações](#)” e responder às perguntas ou indexar as evidências solicitadas.



É possível descobrir quais perguntas foram consideradas incompletas de clicando nos dois ícones ao lado

Solicitação de
Informações

Comentários

Solicitação de informações



3.3 Favor fornecer uma descrição deste processo.

Sim. Conforme definido em nossa Política de Privacidade:
*8. DIREITOS DO TITULAR DE DADOS PESSOAIS

Ao abrir o formulário, é possível percorrer as perguntas que estiverem apresentando o ícone de “Solicitações de Informações”, conforme a figura acima.

Essas solicitações serão inseridas no formato do ícone  ao lado de cada pergunta. Basta clicar nele e a Solicitação de Informação estará numa nova janela que irá se abrir ([ver próxima página](#)).

Cada resposta será avaliada por uma das equipes do **Grupo Icatu**. Em caso de dúvidas ou pendências, a avaliação retornará para **Você** no mesmo ícone.

4.1 *Possui inventário detalhado de ativos de software?
Apresentar Inventário detalhado de todos os softwares licenciados instalados em ativos corporativos.

Implementado Não Implementado

Em planejamento

Campo pedido de informação

Reenviando o formulário



Depois de responder à [Solicitação de Informações](#), é preciso clicar no botão “**Enviar**” para que esta avaliação seja devolvida ao **Grupo Icatu**.

Pedimos que revise o questionário, garanta que ele é o mais completo possível, anexe as evidências em falta e envie o questionário de volta.

titular de dados

Bloco 4 - Perguntas sobre transferência internacional de dados pessoais

< >

Salvar e sair Enviar

SI - Grupo 1 - Avaliação de Fornecedores

Selecione um idioma: ▾

Mostrar: Todas as perguntas ▾

Boas-vindas

Avaliação de Certificado de Segurança >

CIS 01: Inventário e controle de ativos de hardware corporativos >

CIS 02: Inventário e controle de ativos de software >

Bem-vindo a Diligência de Segurança da Informação!

Essa avaliação é baseada no framework do CIS V8 e tem o objetivo de verificar os requisitos mínimos para garantir a segurança da Informação.

Os Controles de Segurança Críticos (CIS) são um conjunto de ações recomendadas para defesa cibernética e fornecem maneiras específicas e acionáveis de prevenção e defesa dos ataques cibernéticos mais comuns e críticos da atualidade e de apoio a conformidade.

O prazo para responder esse formulário é de **7 dias úteis**.

Opções de respostas:

Implementado - *Necessário anexar evidência*
Para os casos em que o controle está implementado na companhia.

Em planejamento - *Necessário informar a data de implementação*
Para os casos em que a implementação do controle está em andamento.

Não implementado

< >

Salvar e sair **Enviar**

Perguntas frequentes



Respondi a diligência de Segurança da Informação. Preciso responder à de Privacidade e GCN? Sim, pois as avaliações possuem objetos distintos, apesar de serem temas parecidos.



Posso repassar a alguém da minha Empresa o email para responder a diligência? O melhor caminho é indicar outra pessoa para responder juntamente com **Você**. Não há limites para a inclusão de respondentes.



Meu Aviso de Privacidade está publicado no site, posso somente incluir o endereço? Pedimos que indexe a evidência. **Você** pode anexar uma impressão da página onde o aviso, com a referência da URL onde ele está hospedado.



Meus artefatos jurídicos (LIA, DPIA, RoPA), políticas e documentos são confidenciais, o que fazer? Anexe uma cópia da capa do documento, do sumário e da data de publicação. Com relação aos artefatos, pode anexar um template ou layout, sem dados pessoais, ou print de seus sistemas. O intuito destas perguntas é avaliar se **Sua Empresa** adota controles e boas práticas para minimizar os riscos, e não avaliar seu teor.

Caso **Você** esteja passando por algum problema técnico e precise que o formulário seja devolvido ou que outras pessoas sejam inseridas, favor entrar em contato com a pessoa do **Grupo Icatu** responsável por sua contratação. Esta pessoa direcionará internamente seus questionamentos e iremos atender **Você** o mais rápido possível.

ICATU
Vida. Pra toda vida.